

CLAIMS

What is claimed is:

1. A method for preventing unauthorized access by a requestor to data sent via computer networks, comprising:
 - a) requesting, from a requesting computer, access to data from a first server;
at said first server:
 - b) determining if said request is a valid request;
 - c) receiving a ticket from a ticket server;
if said request is a valid request:
 - d) providing said ticket identifying said requestor to a second server wherein said data is stored;
 - e) directing said requesting computer to request access to said data from said second server;
at said second server:
 - f) receiving said request from said requesting computer;
 - g) verifying said ticket as identifying said requestor; and
 - h) sending said data to said requesting computer in response to said request.
2. A method according to claim 1 wherein said requesting computer is a client computer.
3. A method according to claim 1 wherein said second server is either of a proxy server and a cache server.
4. A method according to claim 1 wherein said data is encrypted and wherein said providing step d) further comprises said first server providing a decryption key to said second server for decrypting said data.

5. A method according to claim 1 wherein said data is encrypted and wherein providing step d) further comprises said ticket server providing a decryption key to said second server for decrypting said data.

6. A method according to claim 1 wherein said providing step d) further comprises providing said ticket to said second server by way of said client computer.

7. A method according to claim 6 and further comprising said client computer locating said second server using a search engine.

8. A method according to claim 1 wherein said verifying step g) further comprises:

- i) sending said ticket to said ticket server for validation; and
- j) receiving a communication from said ticket server validating said ticket.

9. A method according to claim 1 wherein said sending step h) further comprises embedding a marking into said data prior to sending said data to said client computer.

10. A method according to claim 9 wherein said marking is a digital watermark.

11. A method according to claim 9 wherein said marking is a personalized marking for said requestor.

12. A method for preventing unauthorized transfer of data sent via computer networks, the method comprising the steps of:

instructing a first server to send content to a second server;

notifying a ticket server of said instructions;

validating said instructions at said ticket server;

if said instructions are valid:

notifying either of said servers that said instructions are valid;

sending said content from said first server to said second server;

if said instructions are invalid:

notifying either of said servers that said instructions are invalid;

performing any of:

ignoring said instructions;

corrupting said content; and

discarding said content.

13. A method according to claim 12 and further comprising the steps of:

embedding a marking into said data;

checking the validity of said marking at either of said servers; and

if said marking is invalid, performing any of:

ignoring said instructions;

corrupting said content; and

discarding said content.

14. A method according to claim 12 wherein said validating step comprises validating said instructions in accordance with a policy.

15. A method according to claim 13 wherein said embedding step comprises embedding any of an identification unique to said first server, an identification unique to said second server, routing information, and rule-based information.

16. A method according to claim 12 and further comprising:
said first server receiving an encryption key from said ticket server; and
encrypting said content using said encryption key.
17. A method according to claim 16 and further comprising:
said second server receiving a decryption key from either of said first server and said
ticket server; and
decrypting said content using said decryption key.